icomera

moovbox™

VPN Tunneling

Reference Guide for
Remote Access & Control

©2010 Icomera AB. All rights reserved.

Under the copyright laws, this manual may not be copied, in whole or in part, without the written consent of Icomera. Your rights to the software are governed by the accompanying software licence agreement. Every effort has been made to ensure that the information in this manual is accurate. Icomera is not responsible for printing or clerical errors.

Icomera AB
Vikingsgatan 3
SE 411 04 Göteborg
Sweden
Telephone +46 31 799 21 00
Email support@icomera.com

The Icomera and Moovbox logos are a trademarks of Icomera AB. Moovbox, MoovCare, MoovAdmin, and MoovManage are trademarks of Icomera AB. Other company and product names mentioned herein are trademarks of their respective companies. Mention of third-party products is for informational purposes only and constitutes neither an endorsement nor a recommendation. Icomera assumes no responsibility with regard to the performance or use of these products.

August 2010 Concurrent Firmware – 1.9.0

Contents

Contents 3

1 Introduction to VPN Tunneling 5
- 1.1 Overview . . . 5
- 1.2 Applications . . . 5
- 1.3 Operation . . . 6
- 1.4 System Requirements . . . 7

2 Windows VPN Server Setup 9
- 2.1 Installing & Configuring OpenVPN . . . 9
- 2.2 Setting Up an Ethernet Bridge . . . 11
- 2.3 Starting the OpenVPN server . . . 12
- 2.4 Starting on Boot . . . 12

3 Linux VPN Server Setup 13
- 3.1 Overview . . . 13
- 3.2 Installing using a package manager . . . 13
- 3.3 Installation from source . . . 13
- 3.4 Configuration . . . 14
- 3.5 Setting Up an Ethernet Bridge . . . 16
- 3.6 Starting the OpenVPN server . . . 17
- 3.7 Stopping the OpenVPN server . . . 17

4 Moovbox Setup 19
- 4.1 Configuring VPN Tunneling . . . 19
- 4.2 Configuring Network Time for Authentication Sync . . . 21

5 Running a VPN Connection 22
- 5.1 Testing Your VPN Server . . . 22
- 5.2 OpenVPN for Other Operating Systems . . . 22
- 5.3 Controlling Third Party Devices . . . 23

Appendices 24

A CA Certificate Example 25

B Server Certificate & Key Example 26

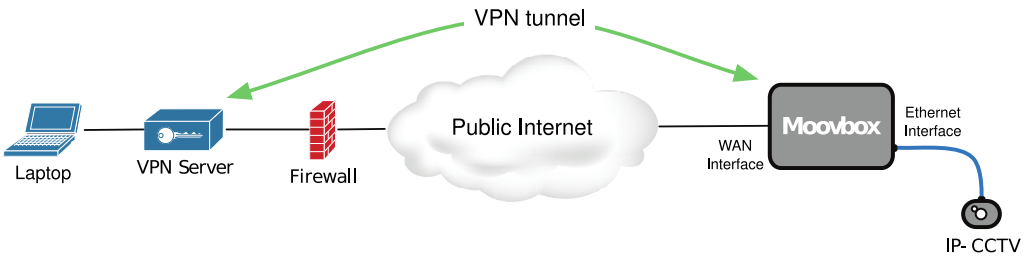
C Client Certificate & Key Example **27**

D DH Parameters Example **28**

E Linux bridge-start script **29**

F Linux bridge-stop script **30**

1 Introduction to VPN Tunneling



1.1 Overview

VPN tunneling enables secure remote access to a specified bridge group on a Moovbox. This will allow configuration changes and firmware upgrades over a wide area network (WAN), even when a static IP address on the Moovbox is not available. VPN tunneling also provides inward bound control of third party devices connected to the Moovbox such as IP-CCTV and DVR systems, telematics equipment, and ticketing machines.

1.2 Applications

The Moovbox M and F Series Broadband Gateways are designed to be used with carrier-class WAN networks, whether 3G UMTS/HSPA, TD-CDMA or WiMAX. Commonly, static IPs are not available when you subscribe to a data service on these types of networks. The VPN Tunneling feature enables you to securely contact and control Moovbox products (and others connected to them) regardless of whether the device has a static or dynamic IP address. For example, a bus may be equipped with a Moovbox M Series using an HSDPA data service, and an IP-based closed circuit TV system and digital video recorder. By creating a VPN tunnel to the Moovbox over the mobile data network, you can control both the Moovbox and the CCTV/DVR equipment remotely. You could also view a live video feed at speeds up to several frames a second, depending on the uplink connection speed available from your mobile carrier and type of video compression used.

Tip: CCTV/DVR systems that support MPEG-4 encoding will provide more efficient streaming of video over a low bandwidth connection.

Note: Icomera does not offer VPN hosting as a service; this Guide shows how Channel Partners and their customers can set up their own VPN tunneling.

1.3 Operation

When tunneling is enabled the Moovbox will act as a VPN client and will attempt to connect to a VPN server defined in the tunneling configuration using certificate authentication. Icomera recommends OpenVPN as a free and quick method for creating a secure tunneling solution. An OpenVPN server needs to be installed and configured on a computer with a public IP address. OpenVPN can be run in the background on system boot allowing for 'always-on' access to multiple Moovbox products and other connected devices. Alternatively OpenVPN can be started and stopped manually as and when needed.

When configured, a Moovbox will attempt to establish a VPN connection as soon as it detects Internet connectivity over its WAN interface. Should the VPN tunnel be disconnected for any reason the Moovbox will attempt to reconnect within one minute.

If you are setting up a VPN system for multiple Moovbox devices, each Moovbox will need its own certificate and a unique IP address, for example:

moovbox1 = 192.168.0.10
moovbox2 = 192.168.0.20
moovbox3 = 192.168.0.30 ...

The IP address range assigned to the Moovbox devices should not conflict with that on your office/corporate LAN. Notice that by spacing the IP addresses of each Moovbox apart, we're allowing for third party devices attached to each Moovbox to be assigned an IP address in a similar range. See page 23 for more information on setting up third party devices.

1.4 System Requirements

- Moovbox with active WAN connection, and firmware v1.9.0 or later
- PC running Windows 2000/XP or higher with both LAN and WAN connections, publicly accessible via the Internet to which the Moovbox can connect via VPN tunneling.

Note: This VPN guide gives instructions for setting up and configuring a VPN server on the Windows and Linux operating systems; MacOS and other operating systems are also supported, see page 22 for more details.

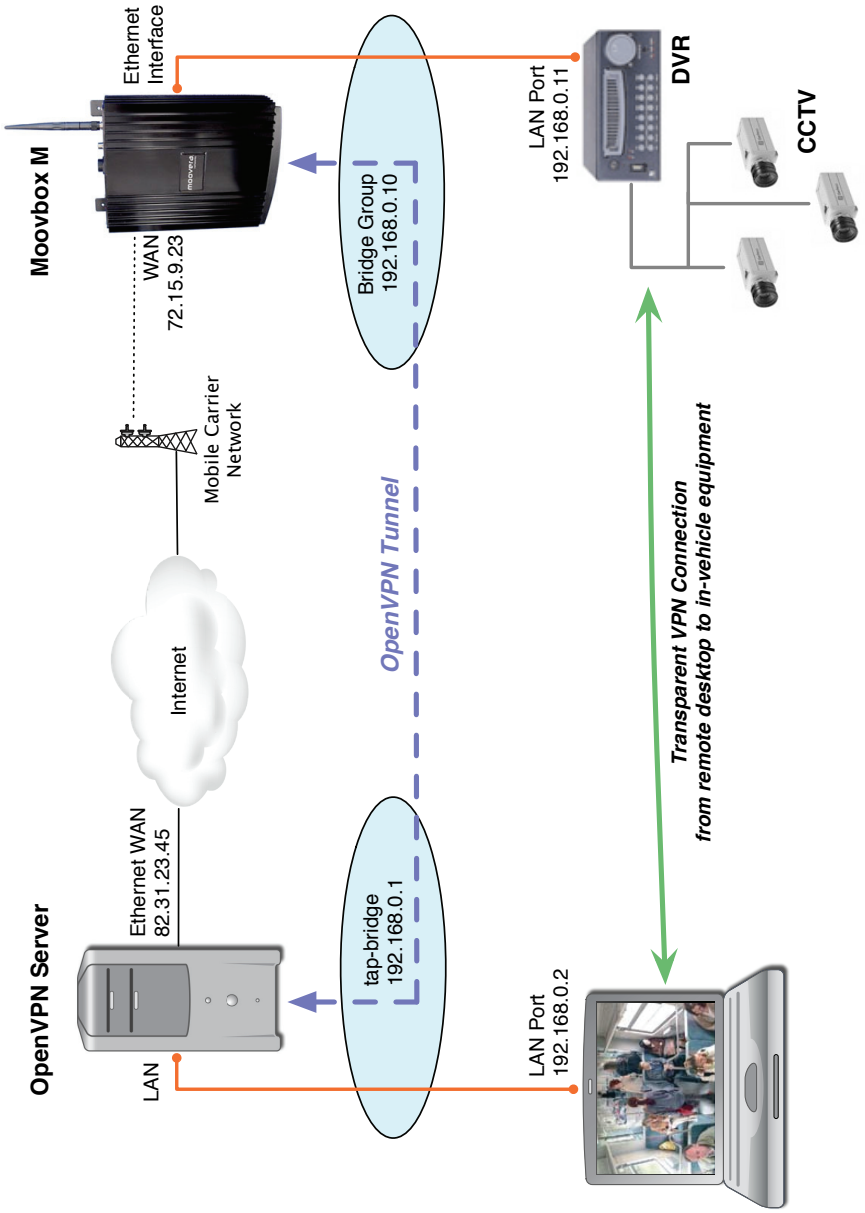


Figure 1.1: Sample Network Diagram

2 Windows VPN Server Setup

2.1 Installing & Configuring OpenVPN

OpenVPN is a full-featured SSL VPN solution which can accommodate a wide range of applications including remote access and site-to-site security. It is a community-supported open source project and is licenced under the General Public Licence (GPL). The latest non-beta version type approved by Icomera for use with Moovbox devices is v2.1.1 (released in December 2009).

Note: The following installation and configuration process requires sufficient technical understanding of using the Windows command prompt and setting up network connections.

1. Download OpenVPN 2.1.1 from:
   `http://openvpn.net/release/openvpn-2.1.1-install.exe`
2. Install on your Windows PC using the default settings
3. Open a command prompt window and type:
   `cd \Program Files\OpenVPN\easy-rsa`↵
4. Type `init-config.bat`↵ to create vars.bat and openssl.cnf files
5. Using notepad, edit the vars.bat file.
   a) Type `notepad vars.bat`↵.
   b) Edit the the following parameters inserting your details:
   ```
   set KEY_COUNTRY=yourcountry
   set KEY_PROVINCE=yourprovince
   set KEY_CITY=yourcity
   set KEY_ORG=yourorganization
   set KEY_EMAIL=youremailaddress
   ```
   c) Save the file and close notepad

6. From the command prompt type the following:
   `vars`↵
   `clean-all`↵ (do not run this when generating additional certificates)

7. Generate a 1024-bit RSA CA Certificate.
   Please refer to Appendix A for an example of this process.

   a) From the command prompt, type `build-ca`↵
   b) Hit Enter until you reach the Common Name line, at which point type `OpenVPN-CA`↵.

8. Generate a server certificate and key.
   Please refer to Appendix B for an example of this process.

   a) From the command prompt, type `build-key-server.bat server`↵.
   b) Hit Enter until you reach the Common Name line, at which point type `server`↵.
   c) At `A challenge password` and `An optional company name` hit enter
   d) At the `Sign the certificate` prompt, type `y`↵.
   e) At the `Commit` prompt, type `y`↵.

9. Generate a client certificate and key for each Moovbox you wish to connect to the VPN.
   Please refer to Appendix C for an example of this process.

   a) At the command prompt, type `build-key moovbox<s/n>`↵ where <s/n> is the serial number of the Moovbox for which you wish to generate a key.
   b) Hit Enter until line Common Name, at which point type `moovbox<s/n>`↵.
   c) At `A challenge password` and `An optional company name` hit enter
   d) At the `Sign the certificate` prompt, type `y`↵.
   e) At the `Commit` prompt, type `y`↵.
   f) Repeat this process for each Moovbox as required

10. The last step is preparing the configuration files is to generate Diffie Hellman parameters.
    Please refer to Appendix D for an example of this process.

    a) From the command prompt, type `build-dh`↵.

The completed files are found in `C:\Program Files\OpenVPN\easy-rsa\keys`

11. Copy the following files `C:\Program Files\OpenVPN\easy-rsa\keys` to `C:\Program Files\openVPN\config`
    `CA.crt`
    `server.crt`
    `dh1024.pem`
    `server.key`
12. From the Icomera Support site, download the server.ovpn configuration file and save to `C:\Program Files\openVPN\config`

Note: The Icomera Support site is located at `http://support.icomera.com`. You will require credentials to gain access. Please contact `moovbox.support@icomera.com` if you do not have a username and password.

2.2 Setting Up an Ethernet Bridge

So that you can communicate with a remote Moovbox at the other end of the VPN tunnel, you must create a bridge between the VPN server and an IP address in the same range as the Moovbox.

1. Select Start > Control Panel > Network Connections
2. Locate the interface created when OpenVPN was installed

Note: This should be called ‘Local Area Connection n’ where n is the highest number. The device name should be ‘TAP-Win32 Adapter V8’.

3. Right click, select Rename and name the interface ‘tap-bridge’.
4. Right click on the tap-bridge interface and select Properties
5. Double-click on Internet Protocol (TCP/IP)
6. Set an IP Address and Subnet Mask in the range used by the Moovbox bridge group to which you’ll be connecting. This will normally be the Default group with the IP range 192.168.0.0/24. Icomera suggests using 192.168.0.1. The Default Gateway and DNS should be left blank.

Note: Don't use 192.168.0.10 as the IP Address as this is would conflict with the default IP address of a Moovbox, unless you have changed it. If setting up VPN tunnels to multiple Moobox devices, refer to the addressing scheme recommended on page 6.

7. Click OK and then OK again to confirm and save the changes.

2.3 Starting the OpenVPN server

You can start OpenVPN on your server in the foreground by going to: `C:\Program Files\OpenVPN\config`, right click on the server.ovpn configuration file, select "Start OpenVPN on this config file". A terminal window will open showing real–time server information including connects, disconnects and errors. If you are prompted by your firewall, click Unblock/Allow.

2.4 Starting on Boot

OpenVPN can be set to start in the background on boot:

1. Go to Control Panel > Administrative Tools > Services
2. Select the OpenVPN service, and right-click on Properties
3. Set the Startup Type to Automatic

3 Linux VPN Server Setup

3.1 Overview

OpenVPN can be installed on Linux using a package management system or by compiling the source code.

3.2 Installing using a package manager

Ubuntu

Note: The following installation and configuration process requires sufficient technical understanding of using the Linux terminal and setting up network connections.

1. Open a terminal (Applications > Accessories > Terminal)
2. Type `sudo apt-get install openvpn`↵

You now need to copy the easy-rsa directory to your home directory to enable you to create the keys

3. Type:
   `cp -r /usr/share/doc/openvpn/examples/easy-rsa/2.0 ~/easy-rsa`↵

3.3 Installation from source

Note: The following section assumes you are comfortable with compiling code in Linux and already have a compiler (gcc) and related tools already installed.

1. Download OpenVPN 2.1.1 from here:
   `http://openvpn.net/release/openvpn-2.1.1.tar.gz`
2. Open a terminal
3. You have to install the lzo development files.
   eg. `sudo apt-get install liblzo2-dev`↵ (Ubuntu)
4. Extract the files
   `tar -zxf openvpn-2.1.1.tar.gz`↵
5. Change to the openvpn source directory
   `cd openvpn-2.1.1`↵
6. Type `./configure --sysconfdir=/etc/openvpn`↵
7. Type `make`↵
8. Type `sudo make install`↵
9. Make the OpenVPN config directory
   Type `sudo mkdir /etc/openvpn`↵
10. Copy the easy-rsa directory to your home directory.
    Type `cp -r ./easy-rsa/2.0 ~/easy-rsa`↵
11. Assuming you didn't get any errors then installation is complete!

3.4 Configuration

1. Open a terminal (if you don't have one open already)
2. Change to the easy-rsa directory by typing
   `cd ~/easy-rsa`↵
3. Open the vars file in an editor. To use gedit type:
   `gedit vars`↵
4. Edit the the following parameters inserting your details:

```
export KEY_COUNTRY=yourcountry
export KEY_PROVINCE=yourprovince
export KEY_CITY=yourcity
export KEY_ORG=yourorganization
export KEY_EMAIL=youremailaddress
```

5. Save the file and close gedit
6. From the terminal, run the following commands consecutively:
   `. ./vars`↵
   `./clean-all`↵ (do not run this when generating additional certificates)
7. This next step generates a 1024-bit RSA CA Certificate. Please refer to Appendix A for an example of this process.
   a) At the command prompt, run `./build-ca`↵
   b) Hit Enter until you are returned to the termal prompt. The window will display a number of parameters pre-filled with the information you entered when you edited the vars file.
8. This step generates a server certificate and key; please refer to Appendix B for the process example.
   a) At the command prompt, run `./build-key-server server`↵.
   b) Hit Enter until the Sign Certificate prompt, then type `y`↵
   c) At the Commit prompt, type `y`↵ to write the file
9. This step generates a client key for each Moovbox you wish to connect to over VPN. Refer to Appendix C for the process example.
   a) At the command prompt, run `./build-key moovbox<s/n>`↵ where <s/n> is the serial number of the Moovbox device you wish to generate the key for.
   b) Hit Enter until the Sign Certificate prompt, type `y`↵
   c) At the Commit prompt, type `y`↵ to write the file
   d) Repeat this process for each Moovbox as required
10. The last step in preparing the configuration files is to generate Diffie Hellman parameters. At the command prompt, run `./build-dh`↵ and the file will be written automatically. See Appendix D for the process example. The completed files are found in the `easy-rsa/keys` path in your home directory.
11. Copy the following files to `/etc/openvpn`
    - ca.crt
    - server.crt
    - dh1024.pem

- server.key

eg. `sudo cp ~/easy-rsa/keys/ca.crt /etc/openvpn/`↵

12. Next you have to create the server configuration file
    a) Type `gksudo gedit /etc/openvpn/server.conf`↵
    b) Enter the following text into the file

```
port 1194
proto udp
dev tap0
mode server
tls-server
dh dh1024.pem
keepalive 10 120
fragment 1400
mssfix
ca ca.crt
cert server.crt
key server.key
```

    c) Save the file and close gedit

3.5 Setting Up an Ethernet Bridge

So that you can communicate with a remote Moovbox at the other end of the VPN tunnel, you must create a bridge between the VPN server and an IP address in the same range as the Moovbox.

1. Open a terminal
2. You need to have installed the bridge-utils package (or equivalent) in your Linux distribution.
    - `sudo apt-get install bridge-utils`↵ (Ubuntu/Debian)
    - `sudo yum install bridge-utils`↵ (RHEL/Fedora)
3. Type `gksudo gedit /etc/openvpn/bridge-start`↵
4. Copy the code from Appendix E into the file

5. Edit the file and set the IP Address and Subnet Mask in the range used by the Moovbox bridge group to which you'll be connecting. This will normally be the Default group with the IP range 192.168.0.0/24. Icomera suggests using 192.168.0.1.

Note: Don't use 192.168.0.10 as the IP Address as this is would conflict with the default IP address of a Moovbox, unless you have changed it. If setting up VPN tunnels to multiple Moobox devices, refer to the addressing scheme recommended on page 6.

6. Save the file and close gedit
7. Make the file executable by typing
   `sudo chmod +x /etc/openvpn/bridge-start`↵
8. Type `gksudo gedit /etc/openvpn/bridge-stop`↵
9. Copy the code from Appendix F into the file
10. Save the file and close gedit
11. Make the file executable by typing
    `sudo chmod +x /etc/openvpn/bridge-stop`↵

3.6 Starting the OpenVPN server

OpenVPN and the bridge can now be started with the following sequence

1. `sudo /etc/openvpn/bridge-start`↵
2. Either: `sudo /etc/init.d/openvpn start`↵ (Ubuntu package)
   `sudo openvpn /etc/openvpn/server.conf`↵ (Self compiled)

3.7 Stopping the OpenVPN server

OpenVPN and the bridge can be stopped with the following sequence

1. Either: `sudo /etc/init.d/openvpn stop`↵ (Ubuntu package)
   `sudo killall openvpn`↵ (Self compiled)
2. `sudo /etc/openvpn/bridge-stop`↵

4 Moovbox Setup

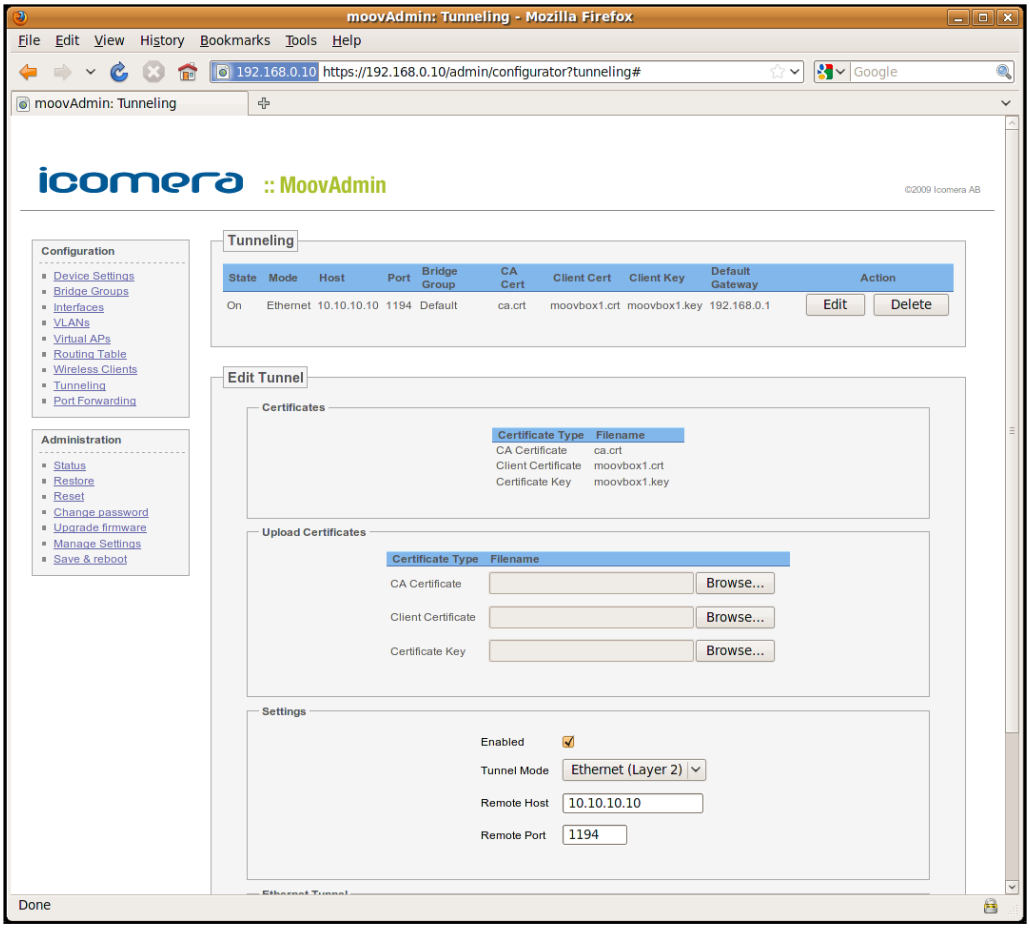


Figure 4.1: The Tunneling screen, shown with one tunnel configured

To complete the setting up of a VPN tunnel, each Moovbox that is to be remotely controlled must be manually configured. This should be done by connecting a PC directly to the Moovbox.

4.1 Configuring VPN Tunneling

1. Connect to the Moovbox, open a browser (Internet Explorer or Firefox preferred) and browse to `https://192.168.0.10` or whatever IP

address schema you have determined for your network

2. Click OK at the security warnings
3. Log in using the admin username and password
4. Select Configuration > Tunneling

Note: Your key files can be found in the following locations:

- Windows: `C:\Program Files\OpenVPN\easy-rsa\keys`
- Linux: `~/easy-rsa/keys` (where `~/` is your home directory)

5. In the Upload Certificates pane, click on the Browse... button next to CA Certificates and choose the `ca.crt` file.
6. In the same pane, click on Browse... next to Client Certificate and choose the `moovbox<s/n>.crt` file where <s/n> is the serial number of this Moovbox

Tip: If you are configuring multiple Moovbox devices for VPN tunneling, be sure not to confuse Client Certificates.

7. In the same pane, click on Browse... next to Certificate Key and choose the `moovbox<s/n>.key` file where <s/n> is the serial number of this Moovbox
8. Ensure the Enabled box is ticked and the tunnel mode is set to “Ethernet (Layer 2)”
9. Enter the Remote host IP address, which is the public IP address of your OpenVPN server. Leave the Remote Port set to 1194 unless the default configuration of your VPN server has been changed.
10. Select the bridge group which will be bridged with the VPN tunnel from the Bridge Group dropdown menu.
11. If the network at your OpenVPN server is bridged to has a default gateway then enter it in the Default Gateway box.
12. Click Add to create the tunneling setup.

4.2 Configuring Network Time for Authentication Sync

The time on the Moovbox and VPN Server need to be synchronized so that they can authenticate correctly. This is accomplished by setting the Moovbox to use Network Time Protocol (NTP).

1. Select Configuration > Device Settings
2. In the General pane, enter a Network Time Server address e.g. pool.ntp.org
3. Select Configuration > Save & Reboot
4. Click on the Save & Reboot button

5 Running a VPN Connection

5.1 Testing Your VPN Server

Make sure the OpenVPN server is started. For Window instructions see section 2.3 (page 12). For Linux instructions see section 3.6 (page 17).

Once a VPN session has been established with your remote Moovbox, open your web browser and try logging into the moovAdmin interface at `https://192.168.0.10` (or whatever IP address you have assigned the device). If the VPN connection is running correctly, you'll be able to access and configure your Moovbox remotely.

Note: A secure VPN connection introduces a certain amount of packet overhead reducing the overall transmission speed of the raw data. It is possible to control a Moovbox remotely over a GPRS connection at under 56Kbps but 300Kbps or faster is recommended especially if you wish to control and view devices downstream of the Moovbox such as IP-CCTV and DVR equipment.

Tip: Check with your WAN service provider to confirm the average upload and download speeds available on their network. Some 3G networks offer symmetrical service e.g. up to 384Kbps in both directions while others offer 384Kbps down and only 64Kbps up. Most first generation HSDPA-enabled (1.8Mbps) networks offer >1Mbps down and 384Kbps up, while 3.6Mbps HSDPA and 7.2Mbps HSUPA networks offer much faster speeds in each direction.

5.2 OpenVPN for Other Operating Systems

As well as Windows and Linux, OpenVPN can also be installed on other operating systems including OpenBSD, FreeBSD, NetBSD, Mac OS X, and Solaris. The configuration is similar to Linux and Windows, and will function in the same way. Please refer to `http://www.openvpn.org` for more information.

5.3 Controlling Third Party Devices

With a secure VPN tunnel open between you and the Moovbox, you can access any third party device attached to the Moovbox Ethernet port and belonging to the same bridge group. By default, the Ethernet interface on the Moovbox is belongs to the Default bridge group.

To set up a third party device that can be remotely controlled:

1. Check the IP and Network Mask of the Default bridge group by going to Configuration > Bridge Groups; an example is shown above.
2. Connect directly to your third party device and assign it an IP address in the same range as the Moovbox Default bridge group e.g. 192.168.0.11. If your VPN server is working with multiple remote Moovbox devices, make sure you do not assign a third party device an IP address already taken by another Moovbox. Also make sure the Network Mask is set correctly.
3. Connect the third party device to the Moovbox Ethernet port. The device should now be accessible remotely on the IP address you assigned it in Step 2.

Appendices

A CA Certificate Example

```
C:\Program Files\OpenVPN\easy-rsa>build-ca
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
....++++++
.......++++++
writing new private key to 'keys\ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [UK]:
State or Province Name (full name) [Kent]:
Locality Name (eg, city) [Sittingbourne]:
Organization Name (eg, company) [Icomera]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:OpenVPN-CA
Email Address [Moovbox.support@icomera.com]:
C:\Program Files\OpenVPN\easy-rsa>
```

B Server Certificate & Key Example

```
C:\Program Files\OpenVPN\easy-rsa>build-key-server.bat
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
..++++++
.....................................++++++
writing new private key to 'keys\.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [UK]:
State or Province Name (full name) [Kent]:
Locality Name (eg, city) [Sittingbourne]:
Organization Name (eg, company) [Icomera]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:server
Email Address [Moovbox.support@icomera.com]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from openssl.cnf
Loading 'screen' into random state - done
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'UK'
stateOrProvinceName   :PRINTABLE:'Kent'
localityName          :PRINTABLE:'Sittingbourne'
organizationName      :PRINTABLE:'Icomera'
commonName            :PRINTABLE:'server'
emailAddress          :IA5STRING:'Moovbox.support@icomera.com'
Certificate is to be certified until Mar 28 14:10:54 2020 GMT (3650 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

C Client Certificate & Key Example

```
C:\Program Files\OpenVPN\easy-rsa>build-key moovbox919999
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
............++++++
.........++++++
writing new private key to 'keys\moovbox919999.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [UK]:
State or Province Name (full name) [Kent]:
Locality Name (eg, city) [Sittingbourne]:
Organization Name (eg, company) [Icomera]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:moovbox919999
Email Address [Moovbox.support@icomera.com]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from openssl.cnf
Loading 'screen' into random state - done
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'UK'
stateOrProvinceName   :PRINTABLE:'Kent'
localityName          :PRINTABLE:'Sittingbourne'
organizationName      :PRINTABLE:'Icomera'
commonName            :PRINTABLE:'moovbox919999'
emailAddress          :IA5STRING:'Moovbox.support@icomera.com'
Certificate is to be certified until Mar 28 14:19:00 2020 GMT (3650 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

D DH Parameters Example

```
C:\Program Files\OpenVPN\easy-rsa>build-dh
Loading 'screen' into random state - done
Generating DH parameters, 1024 bit long safe prime, generator 2
This is going to take a long time
..............+........+.......+.+.......................+..+.......+..........
..................................+...................+.............+..........
.....................................................................................
.......+.........................++*++*++*
```

E Linux bridge-start script

```
#!/bin/bash

################################
# Set up Ethernet bridge on Linux
# Requires: bridge-utils
################################

# Define Bridge Interface
br="br0"

# Define list of TAP interfaces to be bridged,
# for example tap="tap0 tap1 tap2".
tap="tap0"

# Define physical ethernet interface to be bridged
# with TAP interface(s) above.
eth="eth0"
eth_ip="192.168.8.4"
eth_netmask="255.255.255.0"
eth_broadcast="192.168.8.255"

for t in $tap; do
    openvpn --mktun --dev $t
done

brctl addbr $br
brctl addif $br $eth

for t in $tap; do
    brctl addif $br $t
done

for t in $tap; do
    ifconfig $t 0.0.0.0 promisc up
done

ifconfig $eth 0.0.0.0 promisc up

ifconfig $br $eth_ip netmask $eth_netmask broadcast $eth_broadcast
```

F Linux bridge-stop script

```
#!/bin/bash

###################################
# Tear Down Ethernet bridge on Linux
###################################

# Define Bridge Interface
br="br0"

# Define list of TAP interfaces to be bridged together
tap="tap0"

ifconfig $br down
brctl delbr $br

for t in $tap; do
    openvpn --rmtun --dev $t
done
```